The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
10/10/2012

SUBJECT:
Multiple Vulnerabilities in Mozilla Products Could Allow Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Mozilla Firefox, Thunderbird, and SeaMonkey applications, which could allow remote code execution. Mozilla Firefox is a web browser used to access the Internet. Mozilla Thunderbird is an email client. Mozilla SeaMonkey is a cross platform Internet suite of tools ranging from a web browser to an email client. Successful exploitation of these vulnerabilities could result in either an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:
Firefox versions prior to 16
Firefox Extended Support Release (ESR) versions prior to 10.0.8
Thunderbird versions prior to 16
Thunderbird Extended Support Release (ESR) versions prior to 10.0.8
SeaMonkey versions prior to 2.13

RISK:
Government:
Large and medium government entities: **High**
Small government entities: **High**

Businesses:
Large and medium business entities: **High**
Small business entities: **High**

Home users: High

DESCRIPTION:
Multiple vulnerabilities have been discovered in Mozilla Firefox, Thunderbird, and SeaMonkey. The details of these vulnerabilities are as follows:

Miscellaneous memory safety hazards (MFSA 2012-74)

Several memory safety bugs in the browser engine used in Firefox and other Mozilla-based products have been identified. Some of these bugs showed evidence of memory corruption under certain circumstances, and some of these could be exploited to run arbitrary code.

URI-spoofing Vulnerability (MFSA 2012-75)

There is an error when handling the '<select>' drop down menu. This issue can be exploited to display arbitrary content while showing the URL of another site. An attacker can also exploit this issue to cause click jacking attacks.

Security bypass vulnerability when handling 'document.domain' (MFSA 2012-76)

The same-origin policy is not properly enforced. Specifically, the error occurs when handling 'document.domain'. An attacker can exploit this issue to execute cross-site scripting attacks.

Multiple security bypass vulnerabilities in 'nsDOMWindowUtils' methods (MFSA 2012-77)

Several methods of a feature used for testing (DOMWindowUtils) are not protected byexisting security checks, allowing these methods to be called through script by web pages.

Cross-site scripting vulnerability in Firefox for Android (MFSA 2012-78)

When a page is transitioned into Reader Mode in Firefox for Android, the resulting page has chrome privileges and its content is not thoroughly sanitized. A successful attack requires user enabling of reader mode for a malicious page, which could then perform an attack similar to cross-site scripting (XSS) togain the privileges allowed to Firefox on an Android device.

Use-after-free issue (MFSA 2012-79)

A combination of invoking full screen mode and navigating backwards in history could, in some circumstances, cause a hang or crash due to a timing dependent use-after-free pointer reference. This crash may be potentially exploitable.

Denial-of-service vulnerability (MFSA 2012-80)

There is a crash due to an invalid cast when using the *instanceof* operator on certain types of JavaScript objects. This can lead to a potentially exploitable crash.

Security bypass vulnerability in 'GetProperty()' (MFSA 2012-81)

The cross-origin policy is not properly enforced. Specifically, this issue occurs when invoking the 'GetProperty()' function through JSAPI. An attacker can exploit this issue to perform arbitrary code-execution.

Cross-site scripting vulnerability handling the 'location' property (MFSA 2012-82)

User supplied input is not sufficiently sanitized. Specifically, the location property can be accessed by binary plugins through top.location and top can be shadowed by Object.defineProperty as well. This can allow for possible cross-site scripting (XSS) attacks through plugins.

Security bypass vulnerability handling the 'InstallTrigger' object (MFSA 2012-83)

When InstallTrigger fails, it throws an error wrapped in a Chrome Object Wrapper(COW) that fails to specify exposed properties. These can then be added to the resulting object by an attacker, allowing access to chrome privileged functions through script. These issues could allow for a cross-site scripting (XSS) attack or arbitrary code execution.

Spoofing and script injection through location.hash (MFSA 2012-84)

Writes to location.hash can be used with scripted history navigation to cause a specific website to be loaded into the history object. The baseURI can then be changed to this stored site, allowing an attacker to inject a script or intercept posted data posted to a location specified with a relative path.

Multiple use-after-free, buffer overflow, and out of bounds read issues in Address Sanitizer (MFSA 2012-85)

There is a series of security issues using the Address Sanitizer tool in shipped software. Specifically, an out-of-bounds read error affects the 'IsCSSWordSpacingSpace()' function, a use-after-free error affects the 'nsHTMLCSSUtils::CreateCSSPropertyTxn()' function, a heap-based buffer-overflow vulnerability exists in the 'nsHTMLEditor::IsPrevCharInNodeWhitespace()' function, a use-after-free error affects the 'nsSMILAnimationController::DoSample()' function, a use-after-free error affects the 'nsTextEditRules::WillInsert()' function, and a use-after-free error affects the 'DOMSVGTests::GetRequiredFeatures()' function. These issues are potentially exploitable, allowing for remote code execution.

Multiple heap memory corruption issues in Address Sanitizer (MFSA 2012-86)

There is a series of security issues using the Address Sanitizer tool in shipped software. Specifically, a buffer-overflow vulnerability exists in the 'nsCharTraits::length()' function, a heap-based buffer-overflow vulnerability exists in the 'nsWaveReader::DecodeAudioData()" function, a memory-corruption vulnerability exists in the 'insPos' property, and a heap-based buffer-overflow exists in the 'Convolve3x3()' function. These issues are potentially exploitable, allowing for remote code execution.

Use-after-free error in 'nsIContent::GetNameSpaceID()' (MFSA 2012-87)

A use-after-free error was discovered in the IME State Manager code of Address Sanitizer. This could lead to a potentially exploitable crash.

Successful exploitation of these vulnerabilities could result in either an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. Depending on the privileges associated with theuser, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

Upgrade vulnerable Mozilla products immediately after appropriate testing.

Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

Do not open email attachments or click on URLs from unknown or untrusted sources.

Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Mozilla:

http://www.mozilla.org/security/announce/
http://www.mozilla.org/security/announce/2012/mfsa2012-74.html
http://www.mozilla.org/security/announce/2012/mfsa2012-75.html
http://www.mozilla.org/security/announce/2012/mfsa2012-76.html
http://www.mozilla.org/security/announce/2012/mfsa2012-77.html
http://www.mozilla.org/security/announce/2012/mfsa2012-78.html
http://www.mozilla.org/security/announce/2012/mfsa2012-79.html
http://www.mozilla.org/security/announce/2012/mfsa2012-80.html
http://www.mozilla.org/security/announce/2012/mfsa2012-81.html
http://www.mozilla.org/security/announce/2012/mfsa2012-82.html
http://www.mozilla.org/security/announce/2012/mfsa2012-83.html
http://www.mozilla.org/security/announce/2012/mfsa2012-84.html
http://www.mozilla.org/security/announce/2012/mfsa2012-85.html
http://www.mozilla.org/security/announce/2012/mfsa2012-86.html
http://www.mozilla.org/security/announce/2012/mfsa2012-87.html

SecurityFocus:

http://www.securityfocus.com/bid/55856

CVE:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3982
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3983
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3984
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3985
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3986
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3987
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3988
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3989
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3990
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3991
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3992
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3993
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3994
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3995
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4179
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4180
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4181
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4182
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4183
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4185
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4186
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4187
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4188